Grid Security Services Issues

The ESnet PKI Team
Contact: Michael Helm, helm@es.net

A Grid user faces a number of challenges, among them the need to overcome obstacles presented by security services on the Grid. Today the Grid user must acquire an identity token ("X.509 certificate" from a Certificate Authority, and private key), must translate this token into various formats, and probably copy this token to various locations (hosts), in a secure manner. The user must know, and must follow assiduously, an extensive amount of PKI-related security doctrine. The user relies on a complex security infrastructure underlying the Grid, and depends on local and remote system administrators for proper, compatible, and up-to-date installation of this security infrastructure. The user may be a member of a collaborative group, a "virtual organization", representing the user's basic authorization and identity management issues across site boundaries. In this and other ways, the underlying assumptions that drove the development of Grid security have been challenged. The need for account and virtual organization management was not recognized, and the "care and handling" issues associated with the X.509 certificate and private key were not addressed. In general the user experience of PKI in Grids needs substantial improvement, and this concern should be extended to Grid support personnel as well.

The Grid is probably the most diverse PKI (Public Key Infrastructure) ever attempted; it may be one of the largest, and it is certainly the most widespread. Initial success has made the Grid work for a selected and skilled audience, but the challenges facing the Grid user, and the support services on which the user relies, need to be addressed in order to meet the scaling and deployment needs of DOE scientific programs (see "DOE Science Networking Challenge: Roadmap to 2008", pp 22-26). The DOEGrids CA has been in operation for the past two years. It currently has about 1300 certificates, all acquired or refreshed in the past six months. The ESnet PKI project, which developed and deployed this service, has extensive history with DOE Grid projects, a broad perspective on the issues facing them, and unique technical expertise that should be used to meet the challenges facing DOE Grids and Grid users.

We have identified five general areas of difficulty in Grid security that should be addressed. These are: credential storage and management; Virtual Organization management services; Certificate Authority middleware services; policy and federation coordination; and service enhancement and hardening. In consultation with our partners and customers (particularly DOE Science Grid, PPDG, and Globus), we have identified specific projects in each of these areas.

Credential Storage. Many of our customers require a "roaming credential": a convenient, easy to use, and secure method of accessing their Grid identity certificate. A credential store, if properly deployed and with a reasonable UI, could make the user experience much easier. "MyProxy", a proxy credential store now being developed at

NCSA, is highly regarded. Basing our initial work on this technology, we will research the following issues:

1. What are the communities' mobility (roaming) needs?
2. Can MyProxy be operated as persistent, large-scale, distributed infrastructure?
3. Can we improve the security story with our HSM ("Hardware Security Module") {{"HSM" spell out or explain}} technology? Can it pass external security review?
4. How do we move this product towards the standards efforts in credential store (i.e. SACRED)? We will be supporting work with the vendor in this area.
5. How does a secure credential store improve the security profile of Grids, by improving the management of user private keys?

Virtual Organization Services. Virtual organizations (VO), or any project or experiment relying on a Grid, have a basic need to enumerate resources and list members. This forms the foundation of any authorization service. One of our largest customers, the PPDG, has been participating in collaborative work to develop VOMS services with their partners in EDG. They have asked ESnet to pilot a large-scale version of their current VOMS in support of project needs. The VOMS collaborators are also interested in extending their work to include the best features of other technologies like CAS and OGSI. We will answer the following questions:

1. What are the management services needed by each VO?
2. Can we use the existing product to provide persistent, large-scale, distributed VOMS, which can provide the required management services?
3. How can we keep this service aligned with future directions, specifically OGSI AuthZ and Globus development
4. Can this service cooperate with our MyProxy (credential storage) work?
5. What are the underlying, common needs of VO's for account management?
6. How can we interoperate with other, similar technology (ranging from CAS to Shibboleth)?

Certificate Authority Middleware Services. The most serious problem we encountered in the course of deploying DOEGrids CA was the complexity and lack of scalability of the security architecture underlying the most commonly deployed Grid middleware. This middleware is based on OpenSSL, which lacks a distributed services perspective. In the Grid environment, both clients and servers require a complete, well-managed and maintained set of Certificate Authority support files (CA signing certs, policy files, CRL files). Often, this is not robust. Partial or unconscious recognition of this has distorted the environment, contributing to poor decisions: no client deployments, poor CRL policies, inhibiting introduction of needed CA's, &c. We propose three directions to study.

1. OCSP ("Online Certificate Status Protocol") is a simple service that can complement CRL for management of revocation information. This will model the concept of outsourcing infrastructure.
2. Expand to a more general concept: Can we "outsource" all the CA support files? That is, can we move the burden of certificate validation from clients to a reliable, robust, and manageable service? Two emerging international standards, XKMS

("XML Key Management") and SCVP ("Simple Certificate Validation Protocol") will be evaluated. Can either meet this goal? Can we improve the quality of the PKI with them?

3. Research improvements in the existing CRL handling which the middleware vendor has not been able to provide.

Policy Coordination. Grid users, and the virtual organizations and Grids we support directly, require acceptance of DOEGrids certificates in other environments, and also have a need to "manage" the acceptance of certificates from other Grids. We will build on our history of success – e.g. in cross certifying with the European physics community – by answering the following questions:

1. How do we establish management units (such as Policy Management Authorities, VO's, and similar federations) in the Grid? There is value in quantifying the lessons learned from EDG and the DOEGrids PKI.
2. How can we express policies or VO guidance in automated ways? (GGF efforts).
3. How do we set up a North American PMA? DOE representation in a North American PMA will improve coordination between the different PKI's supporting scientific research across the member countries, and make coordination easier with other regional groupings of PKI's in Europe and Asia.
4. How do we support multiple trust domains? We need a vehicle that is less cumbersome and less difficult to review and maintain than the CP/CPS documents, but expresses minimum requirements and agreements, like a service level agreement.

Without this work, there will be no interoperability and there will be no Grid.

Service Enhancement. Our customers have asked us to provide a more general interface to some CA services, including command-line interfaces and email submissions. While some stop-gap measures can meet part of this request, we need to research and develop:

1. A more general way of managing this kind of interface for a general purpose CA infrastructure.
2. Can we find a replacement for current IPlanet CMS, CA software in order to meet community requirements, or do we need to develop in-house PKI solutions like OpenCA? (SunOne/IPlanet has announced "end of life" for their CA product.)
3. Can we improve the security of the CA's trusted agents? We will deploy one or more smart card/token technologies and deploy to trusted agents and administrators of the CA. We will use this small scale deployment to quantify positive and negative features of this technology, and assess more ambitious deployment.